



AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Assignee's Docket No.: 8490.00)
Group Art Unit: 2137)
Serial No.: 09/651,979)
Examiner: Michael Pyzocha)
Filing Date: August 31, 2000)
Title: Portable Terminal)
_____)

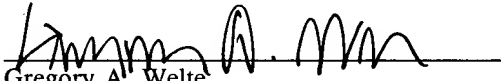
CORRECTED APPEAL BRIEF
A Summary of Argument Begins on Page 25

The fee for this Brief has been paid.

This corrected Brief is submitted in response to the Notice of Non-Compliant Appeal Brief mailed on June 13, 2007.

CERTIFICATE OF MAILING

I certify that this document is addressed to Mail Stop AF, Commissioner of Patents, PO Box 1450, Alexandria, VA 22313-1450, and will be deposited with the U.S. Postal Service, first class postage prepaid, on July 13, 2007.


Gregory A. Welte

1. REAL PARTY IN INTEREST

NCR Corporation.

2. RELATED APPEALS AND INTERFERENCES

None.

3. STATUS OF CLAIMS

Claims 1 - 20 have been cancelled.

Claims 21 - 38 are pending, rejected, and appealed.

09/651,979
Art Unit 2137
Docket No. 8490

4. STATUS OF AMENDMENTS

No Amendments-After-Final have been submitted.

5. SUMMARY OF CLAIMED SUBJECT MATTER

The Invention

Sketch 1, below, illustrates standard conventions which will be used in this explanation. The top of the Sketch illustrates an encryption operation. PLAIN TEXT (eg, a human-readable message) is encrypted into CYPHER TEXT (ie, an encrypted message) using a key K1.

An example of "plain text" would be the phrase

seafood buffet.

This phrase may be encrypted into the cypher text

kbsthoeiwpolsb.

The "i" in the cypher text represents the space character in the plain text (between "d" at the end of "seafood" and the following "b").

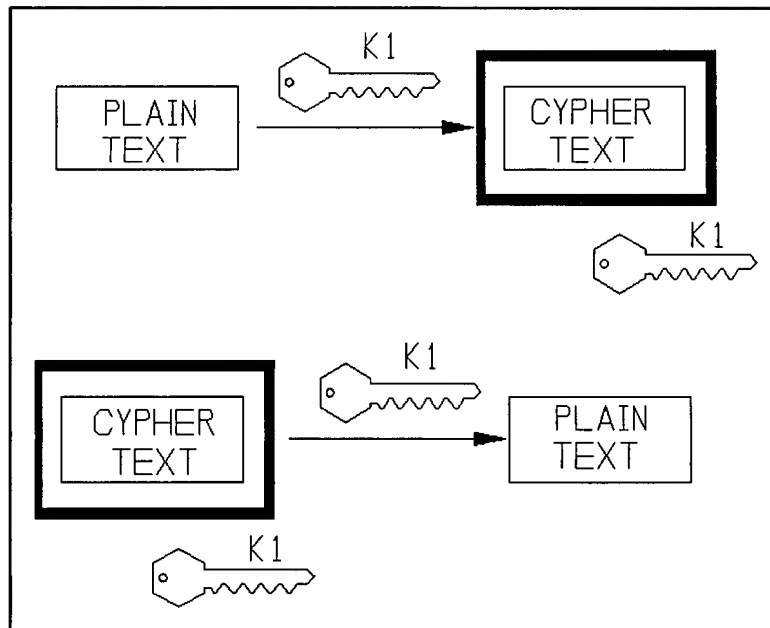
In Sketch 1, the bold box around the CYPHER TEXT represents a lockbox, and the key at the lower right corner of the bold lockbox indicates the key needed to de-crypt the CYPHER TEXT, that is, to "unlock" the lockbox and release the PLAIN TEXT from the lockbox.

The bottom of the Sketch indicates the converse operation. The encrypted CYPHER TEXT is de-crypted using key K1.

Of course, the system can be arranged so that a different key

09/651,979
Art Unit 2137
Docket No. 8490

K2 (not shown), as opposed to K1, is needed to perform the decryption.



Sketch 1

Sketch 2 illustrates processes undertaken by the PDA, Personal Digital Assistant (a portable computer), of the invention. (Specification, page 3, line 1; page 6, lines 17, 18; page 8, lines 17, 18. PDA is shown in Figure 4, item 10.)

First, a SEED is created. (Page 8, line 24.)

(In general, a seed is a starting point, or input, for an algorithm which produces a key. For a given algorithm, different seeds can be used at different times, to produce different keys. An ideal key is a random number, produced by a random number generator. However, it is impossible to produce a truly random number using a digital computer. Nevertheless, digital computers are used to produce keys. Even though these keys are not perfectly random, they are still useful.)

This SEED is derived from data within the memory of the PDA. This data could include the current date, and other data which changes as time progresses. (Page 8, line 25 - page 9, line 2.) In the Sketch, the rectangles represent the data within the memory of the PDA.

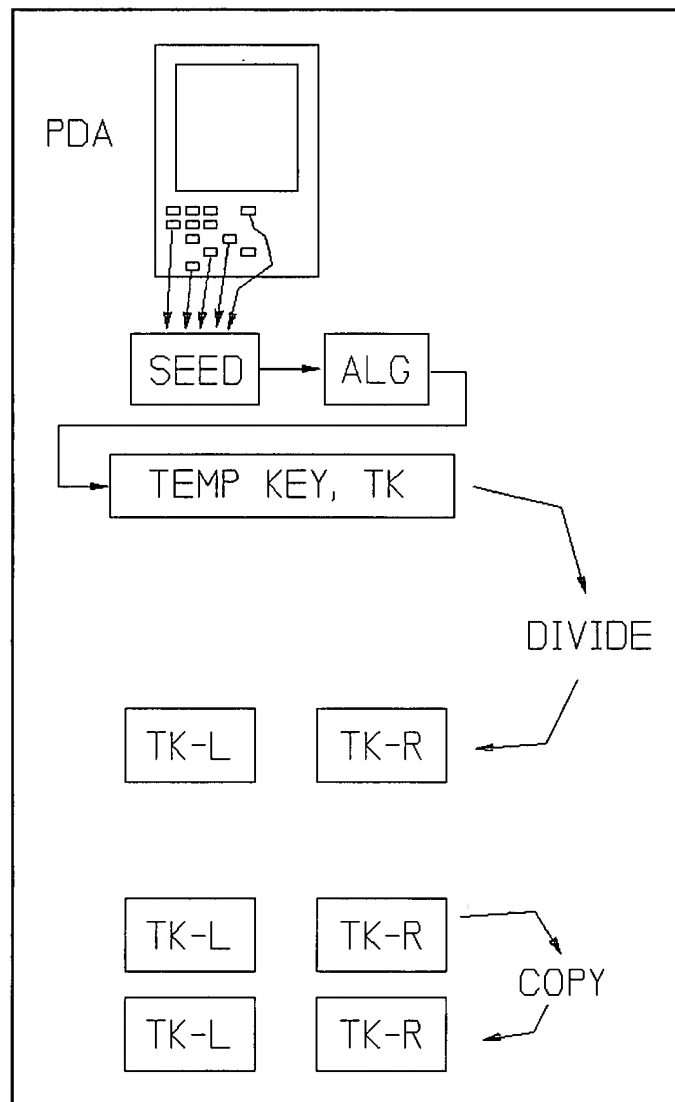
Significantly, this data is not protected: any user of the PDA can gain access to the data. (Page 2, lines 13 - 19. See also page 1, lines 11 - 16; , 27, 28; page 5, lines 13 - 15; page 8, lines 27, 28.)

This data is in "plain view," as it were, for anybody to observe.

09/651,979
Art Unit 2137
Docket No. 8490

Next, an algorithm ALG in the Sketch creates a temporary key, TEMP KEY, or TK. Then TK is divided into two halves, left and right, as shown. (Specification, page 8, line 23 - page 9, line 5. The Specification calls TK a "hash value.")

Finally, the two halves are both copied (conceptually), producing two TK-L's (L: Left) and two TK-R's (R: Right). (Specification, page 9, lines 3 - 7.)



Sketch 2

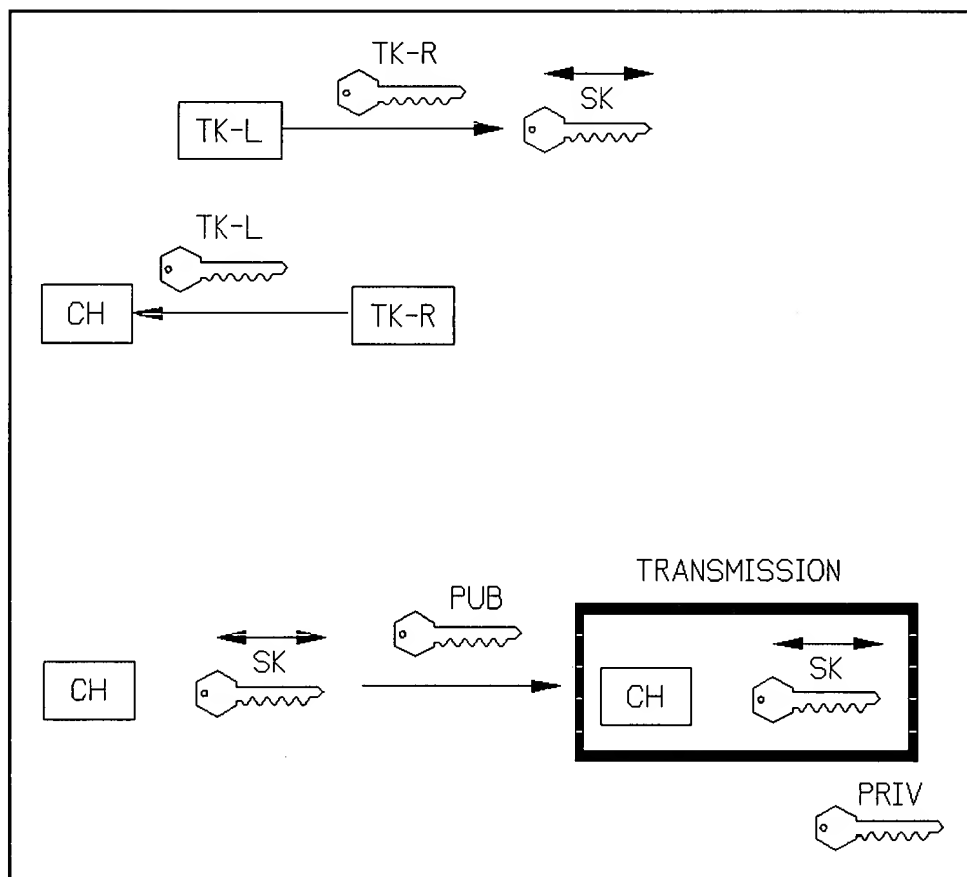
Sketch 3 illustrates further processing within the PDA. TK-R is used as a key to produce a session key SK from TK-L. (In general, a session key is a key which is used for a single "session," and then discarded.) The double arrow indicates that SK is symmetric, meaning that it can both encrypt and de-crypt data. TK-L is used to encrypt TK-R, to produce a challenge CH. (Specification, page 9, lines 6 - 14.)

(In general, a "challenge" is like a password-of-the-day for a clubhouse. You challenge people attempting to enter the clubhouse, by asking for the current password. But the password will be different tomorrow.)

At the bottom of the Sketch, both the newly created CH and SK are encrypted using the public key PUB stored in the PDA. (Specification, page 9, lines 15, 16.) This produces what the Specification calls the TRANSMISSION. (Page 9, line 18.) Note that a private key PRIV is needed to de-crypt the TRANSMISSION. (Specification, page 9, line 20.)

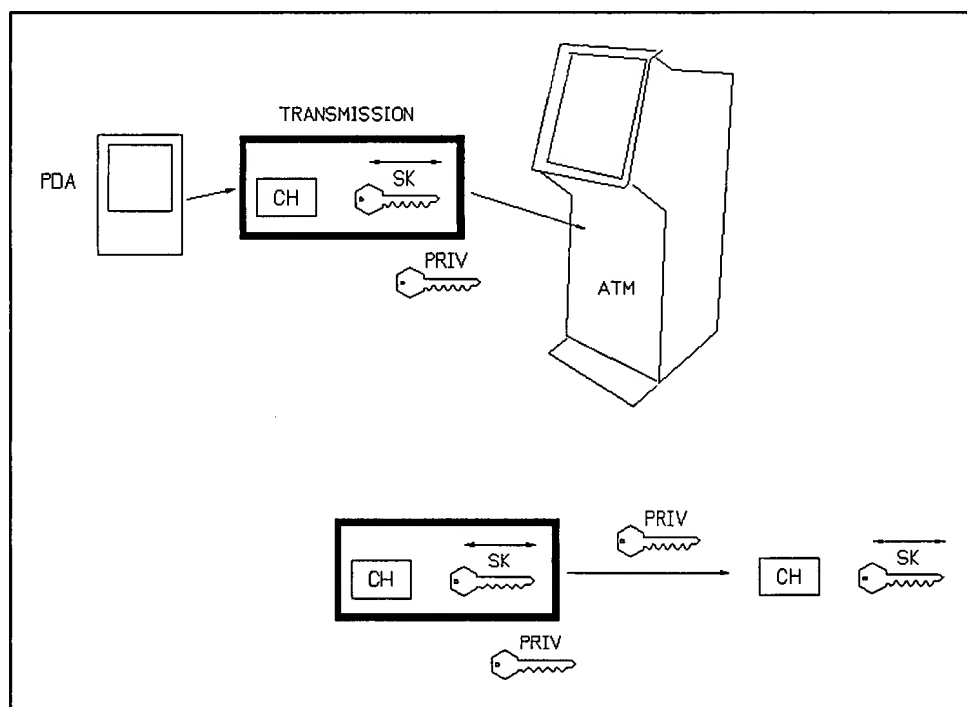
The public key PUB cannot be used for de-cryption, of course, because it is publicly available. If it could be used for the **DE**-cryption, then the **EN**cryption would be pointless. Anybody could defeat the encryption by obtaining the publicly available public key.

09/651,979
Art Unit 2137
Docket No. 8490



Sketch 3

Sketch 4, top, indicates that the PDA transmits the TRANSMISSION to a terminal, such as an ATM. (Page 9, lines 17, 18.) Sketch 4, bottom, indicates that the ATM de-crypts the TRANSMISSION, using its private key PRIV, to recover the challenge CH and the session key SK. (Specification, page 9, lines 18 - 20.)

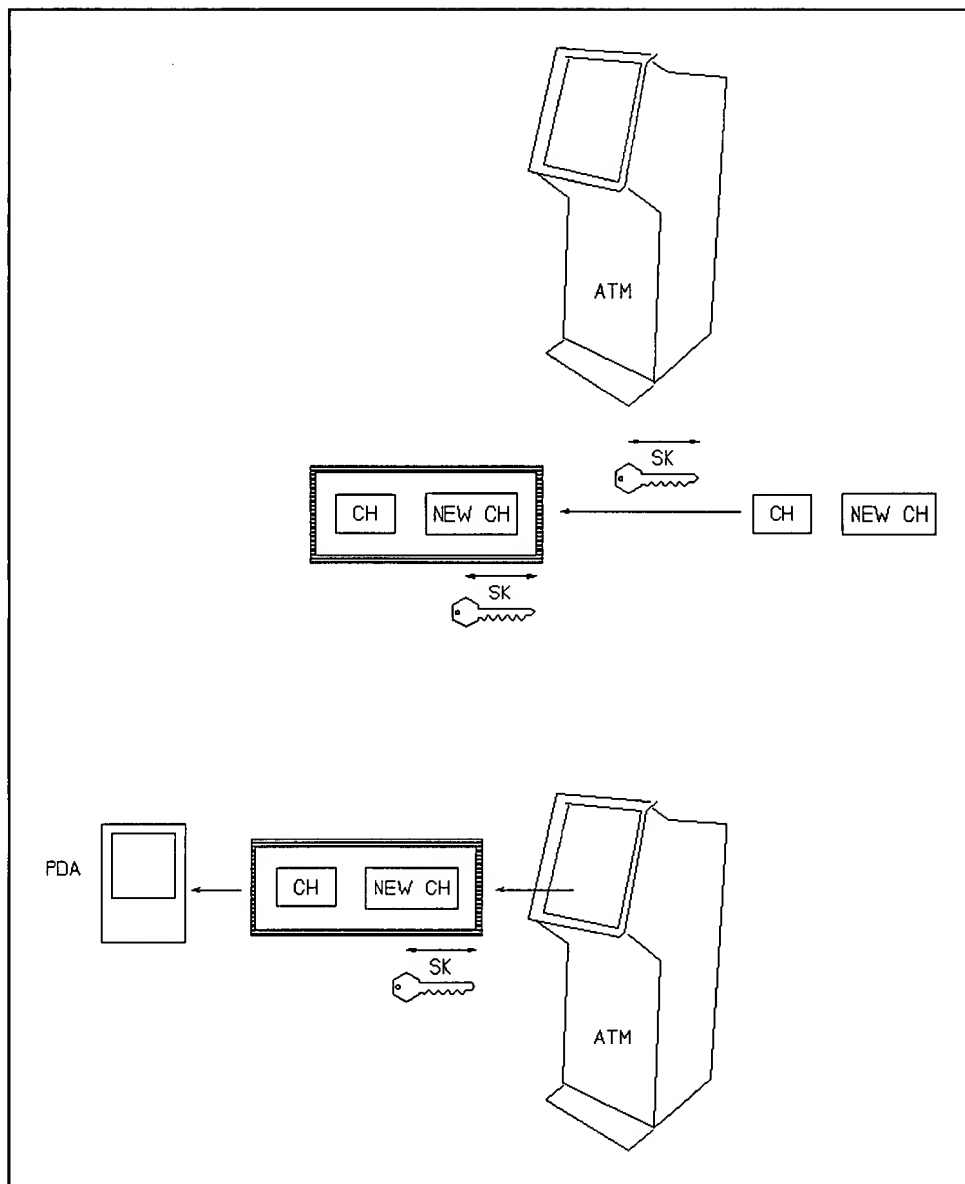


Sketch 4

09/651,979
Art Unit 2137
Docket No. 8490

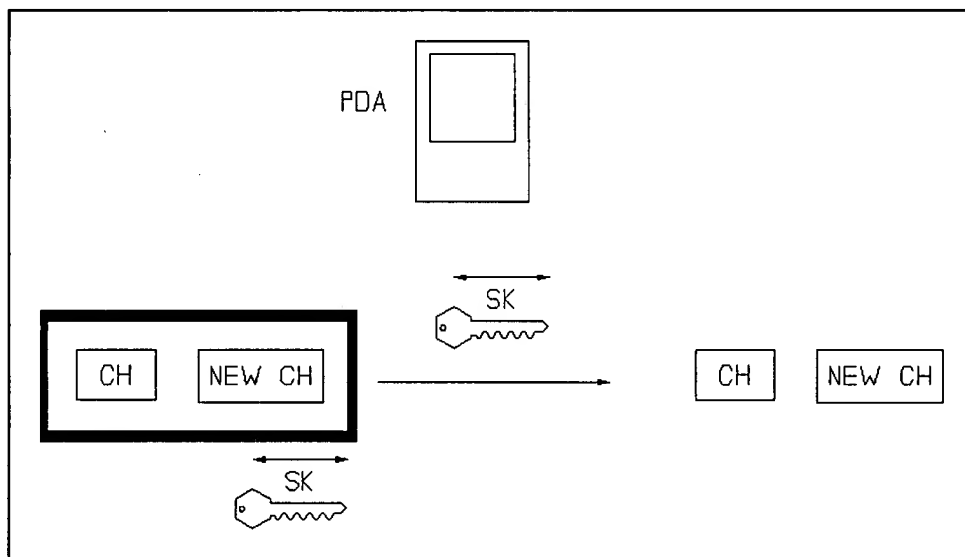
The ATM generates a new challenge NEW CH, based on the challenge CH received. (Specification, page 9, lines 21, 22.) Sketch 5, top, indicates that the ATM encrypts those elements, using the session key SK just received. Sketch 5, bottom, indicates that this encrypted data is transmitted to the PDA. (Specification, page 9, lines 22, 23.)

09/651,979
Art Unit 2137
Docket No. 8490



Sketch 5

Sketch 6 indicates that the PDA de-crypts the data, using the session key SK (created in Sketch 3, top), to recover the challenge CH and the new challenge NEW CH. The PDA can verify whether the ATM is a true ATM through the new challenge NEW CH. If the ATM is an imposter, the PDA can terminate the transaction.



Sketch 6

Identification of "Means"

As required by 37 CFR 41.37(c)(1)(v), Appellant identifies the subject matter supporting the "means" in the claims as follows. Other support is possible.

Claims 30(b) and 32(c) - Figure 2, item 28, and Specification, page 7, line 14 et seq.

Claim 33(a) - Figure 2, item 30, Specification, page 7, lines

3 - 6.

Claim 33(b) - Figure 2, item 34. Specification, page 8, line 25.

Claim 33(c) - Specification, page 8, line 23 et seq.

Mapping of Claim Elements to Specification and Figures

Parenthetical phrases, in **bold typeface**, are inserted into the following independent claims, to identify matter in the Specification and Figures which supports the claim language adjacent said **bold, parenthetical typeface**.

21. A method of operating a portable computer (**portable terminal 10, Figure 1; page 6, line 17 et seq.**), comprising:

- a) storing records of events experienced by the computer in user-accessible memory within the computer (**sub-memory 26 within memory 14 in Figure 1; page 2, lines 13 - 19 page 7, lines 3 - 6 and lines 11 - 13; page 8, line 25 et seq.; page 5, lines 13 - 15**) ;
- b) using one or more of the records as seed for generating plain text of a first session key K1 (**page 2, lines 13 - 19; block 102, Figure 5**); and then
- c) encrypting K1, transmitting K1(encrypted) to an external terminal, receiving an encrypted response from the external terminal, and de-crypting the encrypted

response using the plain text of K1 (page 9, lines 6 - 25; blocks 106, 108, and 110, Figure 5; page 5, lines 4 - 12; page 4, lines 14 - 19.

24. A method, comprising:

a) using a portable computer (portable terminal 10, Figure 1; page 6, line 17 et seq.) to

i) generate a first session key K1, based on one or more seeds derived from data contained in user-accessible memory (sub-memory 26 within memory 14 in Figure 1; page 2, lines 13 - 19 page 7, lines 3 - 6 and lines 11 - 13; page 8, line 25 et seq.; page 5, lines 13 - 15; page 2, lines 13 - 19; block 102, Figure 5);

ii) encrypt K1 into K1(encrypted), using a public key PK (page 9, lines 15 - 17; block 108, Figure 5);

iii) transmitting K1(encrypted) to an external terminal in connection with a first transaction (block 110, Figure 5; page 9, lines 16, 17);

b) using the portable computer to

i) generate a second session key K2, based on

one or more seeds derived from data contained in user-accessible memory (sub-memory 26 within memory 14 in Figure 1; page 2, lines 13 - 19 page 7, lines 3 - 6 and lines 11 - 13; page 8, line 25 et seq.; page 5, lines 13 - 15; page 2, lines 13 - 19; block 102, Figure 5);

ii) encrypt K2 into K2(encrypted), using a the public key PK (page 9, lines 15 - 17; block 108, Figure 5);

iii) transmitting K2(encrypted) to an external terminal in connection with a second transaction (block 110, Figure 5; page 9, lines 16, 17; page 7, lines 12, 13).

28. A method, comprising:

a) maintaining a commercially available Personal Digital Assistant, PDA, which has no secure area for storing an encryption key usable to encrypt outgoing data (page 6, lines 17 - 21; PDA 10, Figure 1; page 5, lines 13 - 15); and

b) using the PDA for encryption and transmission of a message to an external controller in connection with a financial transaction (page 5, lines 21 - 25; page 8,

line 21 - page 10, line 8).

30. Apparatus, comprising:

a) a portable computer (**portable terminal 10, Figure 1; page 6, line 17 et seq.**) having

i) no secure area for storing an encryption key used to encrypt outgoing data(**page 6, lines 17 - 21; PDA 10, Figure 1; page 5, lines 13 - 15**);

ii) system memory, all of which is accessible to a user of the computer (**storage areas 26, 28, Figure 1; page 7, lines 7 - 10**); and

iii) data stored in the system memory, which data changes over time (**page 5, lines 4 - 20**;

b) means (**program 34, Figure 2; page 8, line 23 et seq.**) for

i) utilizing selected changing data in the system memory as a seed for generating a session key K1 (**page 7, lines 11 - 13; page 8, line 23 - page 9, line 14; page 5, lines 4 - 12**);

ii) encrypting K1 into K1(encrypted) (**page 9, lines 15, 16**); and

iii) transmitting K1(encrypted) to an

external terminal (page 9, lines 16, 17).

33. A portable computer (portable terminal 10, Figure 1; page 6, line 17 et seq.), comprising:

- a) means for storing records of events experienced by the computer in user-accessible memory within the computer (memory 14, Figure 1; page 6, lines 18, 19 and lines 22 - 25; page 7, lines 1 - 13; page 5, lines 16 - 20);
- b) means for using one or more of the records as a seed for generating an encryption key (program 34, Figure 2; page 5, lines 6, 7 and lines 16 - 20; page 8, line 25 - page 9, line 2); and
- c) means for using the encryption key in a transaction with an external terminal (programs in memory 28, Figure 2; page 8, line 5 et seq.; page 4, lines 20 - 25).

38. A method, comprising:

- a) storing records of events experienced by a portable computer in user-accessible memory within the computer (memory 14, Figure 1; page 5, lines 13 - 15 and lines 4 - 12; page 7, lines 3 - 6);
- b) using one or more of the records as a seed for generating a session key K1 (page 5, lines 4 - 20; page

8, lines 25, 26);

c) encrypting K1 into K1(encrypted) using a public key
(page 9, lines 6 - 16; block 108, Figure 5);

d) transmitting K1(encrypted) to an external terminal
(page 9, lines 16, 17; block 110, Figure 5);

e) at the external terminal, de-crypting K1(encrypted)
into K1 **(page 9, lines 19 - 21);**

f) encrypting a message M into M(encrypted) using K1 as
key **(page 9, lines 21 - 23);**

g) transmitting M(encrypted) to the portable computer
(page 9, lines 22, 23); and

h) decrypting M(encrypted) using K1 within the portable
computer **(page 9, lines 24, 25; page 5, lines 4 - 12).**

Concise Explanation of Independent Claims

Brief Background on Encryption and Encryption Keys

RANDOMNESS IS DESIRED

A primary goal of cryptography is to create a message wherein every letter (or symbol) occurs with equal frequency. If the 26-letter English alphabet is used, then "A" should occur 1/26 of the time, "B" should occur 1/26 of the time, and so on.

This randomization is desired because, in weak encryption schemes, the original message has statistical properties which can carry over into the encrypted message. For example, "E" is the

09/651,979
Art Unit 2137
Docket No. 8490

most often used letter in English, and the relative frequencies of the other letters is known.

A hacker need only find the symbol occurring most often in the encrypted message, and replace that with "E." A similar replacement is done for all the other symbols.

THE KEY

In performing encryption, a "key" is used. In principle, the key is a number, and the message is another number. (By convention, every letter in the English alphabet is assigned an ASCII code, which is a number. Thus, all text can be treated as a concatenation of these ASCII codes. All text can be treated as a collection of numbers.)

In the encryption process, the key and the message (also called "plain text") are fed as inputs to an algorithm, or equation, which produces another number, namely, the encrypted message, or "cypher text."

The cypher text is de-crypted by another algorithm, using another key (which may, or may not, be the same as the encrypting key), to recover the plain text.

The keys are also desired to be random numbers. They are generated by computers. A starting point is needed for the computer program which generates the keys, and the starting point is a "seed," which is another random number.

The keys produced are generally not truly random numbers, because computers implement "deterministic" processes. The keys are pseudo-random numbers, which are good enough for most encryption operations.

Claim 21

THE SEED

Claim 21 states that, in a portable computer, "events" occurring to the computer are stored in user-accessible memory. The events may be (1) time and date, (2) previous key presses by the user, and so on. These "events" provide data which is somewhat random, but not perfectly so.

Also, as stated, these "events" are stored in user-accessible memory.

These stored "events" are used as a seed to generate a key. Appellant repeats: the seed is not kept secret, but is stored in user-accessible memory. One reason is that the "events" continually change, so that, at any given time, the seed will be different from the seed of an earlier time.

Another reason is that the approach of the invention can be used by portable computers which are not equipped with secret memory. Any portable computer can utilize the invention.

ENCRYPTION

The claim states that the seed is used to generate "plain text" of a key K1. K1 is encrypted, and transmitted to an external terminal. The external terminal generates a "response," which the portable computer receives, and de-crypts, using the plain text of K1 (which the portable computer of course has).

Claim 24

Claim 24 focuses on two situations, such as two banking transactions. Similar encryption processes occur in both, but different data is involved, so that a hacker intercepting a key in one transaction obtains nothing useful as to the second transaction.

In the first situation, a seed is derived from data in user-accessible memory in a portable computer, and is used to produce a key K1. A public key is used to encrypt K1 into K1(encrypted), and the latter is transmitted to an external terminal.

In the second situation, a seed is derived from data in user-accessible memory in the computer, and is used to produce key K2. A public key is used to encrypt K2 into K2(encrypted), and the latter is transmitted to an external terminal.

Claim 28

Claim 28 states that a commercially available PDA (a type of portable computer), having no secure area for storing an encryption

key, is used to encrypt a message in a banking transaction.

Claim 30

Claim 30 recites a portable computer wherein all stored data is available to the user, and some of the data changes over time. Some of the changing data is used as a seed to generate key K1, which is encrypted and transmitted to an external terminal.

Claim 33

Claim 33 recites storing records in user-accessible memory of a portable computer, using the records as a seed for generating a key, and using the key in a transaction with an external terminal.

Claim 38

Claim 38 recites storing events in user-accessible memory of a portable computer, and using the events as a seed for generating a key K1. K1 is encrypted into a public key, and transmitted to an external terminal.

The external de-crypts the public key into K1, and uses K1 to encrypt a message M into M(encrypted), which is sent to the portable computer, which de-crypts M(encrypted) using K1, which the portable computer, of course, has.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

09/651,979
Art Unit 2137
Docket No. 8490

Whether the rejection of claims 21 - 34 and 38 under 35 USC § 103 based on Kawan and Menezes is correct.

Whether the rejection of claims 35 - 37 under 35 USC § 102, based on Yacobi, Menezes and Kawan is correct.

7. ARGUMENT

SUMMARY OF MAJOR POINTS OF ARGUMENT

Claim Element not Shown in References And PTO is Maintaining Inconsistent Positions

Point 1

Claim 21, and others, recite "de-crypting the encrypted response using the plain text of K1."

The PTO has not actually identified the claimed "encrypted response" in the references.

In the Final Action (page 3, end of first paragraph), the PTO finds this recitation at column 9, line 65 - column 10, line 31 of Yacobi. However, the only item at that location which could qualify as the "encrypted response" is a hash value. (A possible exception to this statement is given at the end of this section.)

(A hash value is explained later. A simple type of hash value is a "checksum." For example, if a number is being transmitted, one adds all the digits in the number together, and transmits that sum, which is the checksum, along with the number. For instance, if the number is 4567, then the checksum is $4 + 5 + 6 + 7$, or 22. The recipient adds the received digits together, and compares the result with the checksum received. If they agree, then it is assumed that the number received is the number transmitted.)

Appellant had previously pointed out that the hash value cannot correspond to the claimed "encrypted response." The Final

09/651,979
Art Unit 2137
Docket No. 8490

Action in response to that (eg, page 6, bottom), now asserts that the PTO is not relying on the hash value to show the "encrypted response."

Thus, the Final Action is self-contradictory. On page 3, it states that the hash value shows the claimed "encrypted response." On page 6, it denies that.

Further, if the hash value is not being used to show the claimed "encrypted response," as the Office Action asserts on page 6, then that claim element has not been shown in the prior art.

A possible exception is that the PTO may be relying on the "digital cash" in the cited passage of Yacobi to show the "encrypted response." However, that digital cash is not encrypted. And it has not been shown that the digital cash is "de-crypted" using "K1," as claimed.

Point 2

Even if the hash value is de-crypted, it is not de-crypted "using the plain text of K1."

The Office Action treats a "session key" in Yacobi as K1 of the claim. (Final Action, page 2, last paragraph.)

Yacobi states that the hash value is encrypted using the bank's private key. (Column 10, lines 22 - 25.)

But the "session key" cannot de-crypt the hash value, which was encrypted using the private key.

The hash value is not de-crypted "using the plain text of K1."

No Reason for "Portable Computer" to De-Crypt Hash Function

Claim 21 states that the "portable computer" de-crypts the "encrypted response."

Yacobi does not state that his portable computer de-crypts the hash value, and the PTO has not identified such a statement.

Further, there is no reason for Yacobi's portable computer to de-crypt the hash value. The hash value is used to verify the digital cash which Yacobi downloads to the customer's portable computer. The merchant at which the customer spends the digital cash wants to verify the digital cash. But the customer himself has no need to do that. And Yacobi does not state that the customer does that, in the customer's portable computer.

PTO Makes Erroneous Statement

In an attempt to rebut Appellant's preceding arguments, the Final Action asserts that, in Yacobi, "**every message . . .** is encrypted with the session key." (Page 6, first full paragraph; page 7, first full paragraph.) Thus, the Final Action concludes that, since the "response" is necessarily encrypted, it is necessarily de-crypted "on the other end of the channel." (Final Action, page 6, first full paragraph.)

However, Yacobi does not state that "every message" is

09/651,979
Art Unit 2137
Docket No. 8490

encrypted. The PTO has provided no evidence in support of its assertion.

Further, it appears that the digital cash (Column 10, line 8 et seq.) is not encrypted, which is directly contrary to the PTO's statement.

Further still, Yacobi states that the "hash value" (discussed below) is encrypted using the bank's "private key," not the session key. (Column 10, lines 22 - 25.) That fact directly contradicts the PTO's assertion.

Thus, at a minimum, the PTO's premise ("every message . . . is encrypted . . .") is unsupported, and therefore does not support its conclusion. And "every message" is not encrypted using the "session key," as just shown.

Even if References are Combined, Claimed Invention not Shown

Yacobi discusses numerous keys.

1. Those manufactured into the wallet.
(Column 8, lines 50 - 52.)
2. The "signing keys." (Column 9, lines 4, 5.)
3. The session key. (Column 9, line 47.)
4. The public exchange key. (Column 9, line 50.)
5. The private exchange key. (Column 9, line 55.)

6. The private signing key. (Column 10, line 24.)

7. The different private signing keys.
(Column 10, line 26.)

The claim states that a specific "seed" is used to generate key K1. The PTO states that Menezes shows this "seed."

However, no teaching has been given explaining why the "seed" of Menezes should be applied to a specific one of the keys of Yacobi listed above.

Therefore, the claimed invention has not been shown in the references, even if combined.

The PTO has done nothing more than assert that Menezes should be combined with Yacobi, but has not explained what is combined with what in each reference. Thus, the PTO has not shown the claimed invention in the combination.

No Teaching Given for Combining References

Point 1

The rationale given for combining the references is that the combination provides "a random bit sequence for a key." (Final Office Action, page 3, fourth full paragraph.)

However, in the context of obviousness, this is a meaningless statement. It is well known that **ALL KEYS** should be random bit sequences. That fact, which applies to all keys, does not, as a

09/651,979
Art Unit 2137
Docket No. 8490

matter of logic, lead to the combination of references.

Stated another way, each reference, by itself, wants a random bit sequence for its key. Why does that mean that the references should be combined together ?

It does not.

Point 2

The rationale given is technically erroneous. As explained near the end of this Brief, in the rebuttal to statements in the Final Action, Page 8, First Full Paragraph, it is **impossible** to attain a truly random number using a computer.

The combination of references involves computers.

Computers cannot achieve "a random bit sequence for a key."

The rationale is erroneous, and cannot be used.

Thus, **no teaching at all** has been given for combining the references.

Comment 1

Not all points made in this Summary are elaborated below. Some are considered self-explanatory.

These points apply to most, if not all, the remaining claims.

Comment 2

This Brief, for purposes of simplifying the argument, states

09/651,979
Art Unit 2137
Docket No. 8490

that the hash value of Yacobi is encrypted using the bank's private key. (Yacobi, column 10, line 22 et seq.)

That is, this Brief is arguing that, even if the operation in Yacobi qualifies as encryption, the claims are still not shown.

However, Yacobi actually refers to "digitally signing" the hash value "by operating with the bank's private signing key." That may not be true encryption. If not, Appellant has not admitted that operation to be true encryption.

END SUMMARY

09/651,979
Art Unit 2137
Docket No. 8490

RESPONSE TO OBVIOUSNESS REJECTIONS OF
CLAIMS 21 - 34 and 38

CLAIM 21

Even if References Combined,
All Claim Elements not Found - Part 1

Claim 21(c) recites "de-crypting the encrypted response using the plain text of K1." This has not been shown in Yacobi. The Office Action only asserts that Yacobi shows de-crypting a response from the terminal. (Office Action, page 3, end of first paragraph.)

The Office Action does not show that the "plain text of K1" is used in that de-cryption, as claimed.

Therefore, even if the references are combined, the claim recitation is not found. No de-cryption using "plain text of K1" as key has been shown. MPEP § 2143.03 states:

To establish prima facie obviousness . . . **all the claim limitations** must be taught or suggested by the prior art.

This applies to claims 26(c)(ii), 32(c)(ii), and 38(h).

09/651,979
Art Unit 2137
Docket No. 8490

**Even if References Combined,
All Claim Elements not Found - Part 2**

Background

HASHING FUNCTION

Appellant will first explain some principles involving digital cash, and then explain why Yacobi's use of digital cash does not show the claim recitations.

First, a generalized "hash function" will be explained. Assume that a message contains four decimal digits, as shown in Sketch 1, below.

MESSAGE	HASH VALUE
0000	
⋮	
1234	$1 + 2 + 3 + 4 = 10$
⋮	
2134	$2 + 1 + 3 + 4 = 10$
⋮	
3124	$3 + 1 + 2 + 4 = 10$
⋮	
4123	$4 + 1 + 2 + 3 = 10$
⋮	
9999	

Sketch 1

09/651,979
Art Unit 2137
Docket No. 8490

The message has 10,000 possible values, running from 0000 to 9999.

A hash function generally is a type of abstract of the message. In Sketch 1, the hash function is the sum of the digits in the message. The sum is called the "hash value." For the message 0000, the sum is zero. For the message 9999, the sum is 36, and so on.

Two points are significant here. One, for a hash function such as this one, which produces a hash value which is smaller than the message, **different** messages can produce the **same** hash value. That is, the hash value is not unique to the message.

The examples in Sketch 1 illustrate this non-uniqueness: the messages 1234, 2134, 3124, and 4123 all produce the same hash value of 10. Other examples are 0505, 5050, etc.

Thus, a given message's hash value is not unique. Different messages can produce the same hash value.

The second point is that the hash function is not reversible, so that the content of the message is not carried over into the hash value. Only some characteristic of the message (the sum of the digits in this example) is carried over into the hash value.

Consequently, the hash function cannot be processed to deduce the message which produced it. The examples in Sketch 1 again illustrate the point: if you are given the hash value of 10, you do not know which of the many messages produced that hash value.

09/651,979
Art Unit 2137
Docket No. 8490

Thus, a hash function is not a type of translation. In contrast, encryption is a type of translation: the original message can be derived from the cypher text.

Therefore, these two points illustrate the fact that a hashing function is not, in general, equivalent to encryption.

-- The hash value is not unique to the message. This prevents reversibility, or deriving the message from the hash value. Decryption of the hash value is not possible.

-- The hash function does not translate the message into a new form. Thus, the hash value cannot be re-translated into the message.

Of course, it may be possible to define a function which is reversible, and call it a hash function. However, such a function has not been shown in the references.

DIGITAL CASH

The phrase "ten dollars, unique serial number, bank ABC" could be used as digital cash. "Ten dollars" is the value of the digital cash, "serial number" is a unique number assigned to that piece of cash, and "bank ABC" is the bank issuing the cash.

To spend the digital cash, one transfers the phrase to a merchant, who then contacts bank ABC, and tells ABC the serial number. ABC verifies that serial number, and then authorizes ten

09/651,979
Art Unit 2137
Docket No. 8490

dollars for a purchase.

However, a dishonest person could alter the phrase. Further, it may be desirable to eliminate the step of contacting ABC bank to verify the phrase.

To these ends, a hash value of the phrase can be derived. The hash value is inserted into the phrase, which now reads

ten dollars, unique serial number,
bank ABC, hash value.

The hash value could be the sum of the ASCII values of the characters in the phrase.

When validation of the digital cash is requested, the merchant, or the bank, computes a hash value for the phrase, using the same hash function. If the hash value produced matches the hash value contained in the phrase, the phrase is assumed to be authentic, and no alteration is assumed to have occurred.

However, a dishonest person can alter the phrase, compute the hash value for the altered phrase, and insert that new hash value into the phrase. Now the phrase could read:

1,000 dollars, unique serial number,
bank ABC, new (false) hash value

To prevent this, the hash value can be encrypted, using a private key which only bank ABC possesses, or only merchants possess, or both. Thus, the phrase becomes

09/651,979
Art Unit 2137
Docket No. 8490

ten dollars, unique serial number,
bank abc, hash value(encrypted)

Since the dishonest person lacks the private key, he cannot generate a false hash value, and then properly encrypt it.

Greater detail concerning hash functions and digital cash can be found at the following web sites:

[www.iusmentis.com/technology/encryption/crashcourse/
digitalsignatures](http://www.iusmentis.com/technology/encryption/crashcourse/digitalsignatures)

www.aci.net/kalliste/cryptnum.htm

Application to Yacobi

Claim 21(c) recites "de-crypting the encrypted response using the plain text of K1." The Office Action cites Yacobi, column 9, line 65 - column 10, line 31 to show this.

POINT 1

However, that passage of Yacobi shows generating digital cash by a bank. The digital cash is described in column 10, lines 14 - 16, and an example of a 550-bit number is given.

Yacobi then states that a hash value is derived from the 550-bit number. The bank then encrypts the hash value, using its private key. (Column 10, lines 22 - 25.) The encrypted hash value is then transferred to the customer's electronic wallet. (Column 10, lines 32, 33.)

Appellant points out that no de-cryption occurs in this passage of Yacobi. Claim 21(c) recites a de-crypting process.

Thus, the encrypted hash value of Yacobi does not correspond to the "encrypted response" in claim 21(c). That encrypted hash value is not de-crypted, as claimed.

POINT 2

Claim 21(c) recites "de-crypting the **encrypted response**." No "encrypted response" is shown in this passage of Yacobi. The Office Action relies on a hash value in Yacobi to show the claimed "encrypted response." However, as explained above, a hash value is not, in general, an encrypted response. A hash value cannot be de-crypted.

Nor is "de-crypting" of any "encrypted response" shown in this passage. Nor is "de-crypting" of even a (non-encrypted) "response" shown in this passage.

Therefore, Appellant submits three claim elements are missing from Yacobi:

- 1) The claimed de-cryption..
- 2) The claimed encrypted response.
- 3) The claimed de-cryption of an encrypted response.

It could be that the PTO is relying on the digital cash (or electronic cash) to show the "encrypted response." However, the

09/651,979
Art Unit 2137
Docket No. 8490

PTO has not shown that the digital cash is encrypted, nor that the customer's portable computer de-crypts the digital cash. And Yacobi discusses neither of these two things.

Further, the customer has no need to de-crypt the digital cash (even if encrypted). The merchant where the customer spends the digital cash would perform any de-cryption.

POINT 3

Claim 21 recites "de-crypting the encrypted response using the plain text of K1." As just explained, the Office Action treats the hash value of digital cash in Yacobi as the "encrypted response." There is no de-cryption of that hash value. Nor is there de-cryption using K1 as a key.

POINT 4

The Office Action treats the "session key" in Yacobi as the claimed key K1. The Office Action asserts that Yacobi uses that "session key" to encrypt a message which a wallet transmits to an ATM. The Office Action asserts that the ATM then uses the same "session key" to de-crypt that message. (Column 9, lines 47 - 61.)

However, that "session key" is not involved in Yacobi's encryption of the hash value of the digital cash. (The bank's private key is sued.) Therefore, the "session key" cannot be involved in any de-cryption of the hash value. Consequently,

09/651,979
Art Unit 2137
Docket No. 8490

Yacobi's "session key" (supposedly the claimed K1) does not de-encrypt the hash value (supposedly the encrypted response).

De-encryption of an "encrypted response" using the plain text of K1 is not found in Yacobi.

POINT 5

Under the terms of the claim, the operations of claim 21(c) are performed in the "portable computer." However, any processing of the hash function of the digital cash in Yacobi is done **outside** the electronic wallet. The processing is done by a merchant receiving the digital cash. Thus, even if Yacobi de-encrypts the hash function of the digital cash (which has not been shown), that operation occurs **outside** the electronic wallet.

Further, it would make no sense to perform Yacobi's de-encryption **within** the wallet, because any de-encryption is designed to verify the digital cash. It makes no sense, and there is no need, for the owner of the wallet to verify his own digital cash.

Thus, any de-encryption of the hash value in Yacobi (if de-encryption occurs) occurs **outside** the electronic wallet. That does not correspond to the claim.

Even if References Combined, All Claim Elements not Found - Part 3

Menezes is cited for the proposition of using changing data in a computer as a seed for a key.

Even if that proposition is combined with Yacobi, the PTO has not shown that the specific operation of claim 21 is attained. For example, it has not shown that Menezes' seed is used to generate K1 of the claim, that K1 is encrypted, transmitted etc.

From another point of view, Yacobi discusses several types of key:

1. Those manufactured into the wallet.
(Column 8, lines 50 - 52.)
2. The "signing keys." (Column 9, lines 4, 5.)
3. The session key. (Column 9, line 47.)
4. The public exchange key. (Column 9, line 50.)
5. The private exchange key. (Column 9, line 55.)
6. The private signing key. (Column 10, line 24.)
7. The different private signing keys.
(Column 10, line 26.)

No teaching has been given explaining why the seed of Menezes should be applied to a specific one of these keys.

INTERIM CONCLUSION

Appellant submits that the rejection of claim 21 cannot stand, for at least the following reasons.

-- Yacobi shows no de-crypting of an encrypted response using key K1.

-- Yacobi's hash value of the digital cash cannot qualify as the claimed "encrypted response."

-- The Office Action treats the "session key" in Yacobi as key K1. For that to be so, then Yacobi's "session key" must be used to de-crypt the hash value. That is not done.

-- The Office Action has not explained which of the many keys in Yacobi should use the seed of Menezes, and why.

No Teaching Given for Combining References

The rationale given for combining the references is that the combination provides "a random bit sequence for a key." (Final Office Action, page 3, fourth full paragraph.) However, several problems exist in this rationale.

Problem 1

This rationale is merely a restatement of a well known fact in cryptography, namely, that an ideal key is a random bit sequence. Thus, since both references are interpreted as speaking to a person skilled-in-the-art, and since they both discuss keys,

they both are interpreted in light of this well known fact.

Consequently, both references impliedly state, if they do not explicitly state, that their keys are random bit sequences.

Therefore, the statement does not lead to a combination of the references. Each reference, by itself, teaches using a random bit sequence, for its own purposes. The other reference is not needed to achieve those purposes.

Problem 2

The Office Action cites Menezes as stating that the starting point for a key can be user-accessible data which is stored in the user's computer. Even if that be true, Menezes discusses other sources of a random number for use in generating a seed. (See page 172.) Those other sources do not show the claimed subject matter.

Therefore, no teaching has been given in favor of selecting one approach in Menezes, as opposed to other approaches, and then combining the one selected approach with Yacobi.

Problem 3

Claim 21(a) states that the "records" are stored in "user-accessible memory." Claim 21(b) states that the "seed" for key K1 is generated from those "records."

Thus, any user of the claimed "portable computer" has access to the "records." That is contrary to Menezes' teachings.

Menezes, in section 5.2, states that "A random bit generator requires a . . . source of randomness." Under claim 21, the "source of randomness" would be the claimed "records." Thus, under claim 21, the "source of randomness" would be "user-accessible."

But Menezes' section 5.2 also states, "The generator must not be subject to observation." Menezes is contrary to storing the "records" in "user-accessible memory," as claimed.

Thus, Menezes teaches against claim 21.

Also, Menezes' section 5.2(ii) lists some events which may be similar to those in the "records" of claim 21. But Menezes states that an "adversary" should be prevented from "observing" those events. (Menezes, section 5.2(ii), fourth sentence.) Again, that is opposite to claim 21, which states that those events are stored in "user-accessible memory."

Therefore, Menezes teaches against the recitation of claim 21 regarding user-accessibility to the records used for the seed. The Office Action has provided no rationale which overcomes Menezes' contrary teaching.

Problem 4

At least two possibilities exist in Menezes.

POSSIBILITY 1

One is that Menezes

- 1) stores parameters in memory and then
- 2) later reads the parameters, and
- 3) then applies the parameters as inputs to an algorithm, to produce a key.

POSSIBILITY 2

Another possibility is that Menezes eliminates steps (1) and (2), above, and applies the parameters directly to the algorithm, to produce a key.

That is, the parameters are not stored and then read from storage.

His page 172, "(ii) Software-based generators," provides an example. He merely observes currently existing parameters (eg, system clock), and uses the observed parameters as the seed.

As a simple analogy, Menezes can watch a baseball game, and use

- 1) the current jersey-numbers of the players on-base,
- 2) the current score,
- 3) the current inning number, and
- 4) the current time-of-day

as his seed. He need not store anything in memory. He merely observes events.

ANALYSIS OF POSSIBILITIES

If the latter possibility occurs (no storage, only observation), then the recited storage of claim 21(a) is not found in Menezes.

The PTO has not shown which possibility occurs in Menezes. Therefore, claim 21(a) has not been shown in the references, even if combined.

Problem 5

Menezes, page 172, discusses at least two approaches to generating a random number: (1) a hardware-based approach, and (2) a software-based, computational, approach. The first approach is clearly irrelevant to Appellant's claims, and does not show the claimed subject matter.

No teaching has been given in favor of eliminating Menezes' first approach, and selecting Menezes' second approach.

Further, Menezes expressly states that the second approach is "more difficult" than the first. (First sentence of section entitled "(ii) Software-based generators.") Thus, Menezes teaches away from the second approach, thereby teaching away from the invention.

Further still, the section entitled "(ii) Software-based generators" repeatedly states that the parameters used to generate the random number must be kept secret. That teaches away from the

claim recitation that the seed is derived from "user-accessible memory."

Problem 6

A problem similar to Problems 4 and 5 applies to Yacobi.

Yacobi shows at least two implementations, an "anonymous" and a "non-anonymous" implementation. The Office Action combines the latter with Menezes.

But no teaching has been given for selecting the latter over the former.

Conclusion

No de-cryption as in claim 21(c) is found in Yacobi. Yacobi encrypts a **hash value**. The user in Yacobi does not **de-crypt** the encrypted hash value, because the user has no need to do so.

No de-cryption of a "response" as in claim 21(c) is found in Yacobi.

No de-cryption "using the plain text of K1" as in claim 21(c) has been shown in Yacobi.

No teaching has been given for combining the references. The rationale given is merely a well-known fact, or goal, in the art of cryptography. The references need not be combined to attain that goal. And Menezes, by himself, expressly states that the goal (random number for a seed) is desirable.

REMAINING CLAIMS

The discussion of claim 21 applies to the remaining claims in this group. Appellant further makes the following comments regarding selected claims in this group.

Claims 22 and 23

Claims 22 and 23 are considered patentable, based on their parents.

Claim 24

Claim 24 recites producing keys from seeds derived from user-accessible memory. As explained above, Menezes teaches contrary to this.

Claim 24 also recites encrypting two keys, **using a public key**, and transmitting the encrypted keys to an external terminal. This has not been shown in the references. The Final Action, page 3, bottom, treats claim 24 as setting forth a repetition of processes of claim 21. However, claim 21 does not recite the **public key**.

In addition, as explained above, no valid teaching has been given for combining the references. "Generating a random bit sequence for a key" (Final Action, page 3, fourth full paragraph) does not act as a teaching.

And the references, either combined or individually, **DO NOT**

09/651,979
Art Unit 2137
Docket No. 8490

generate "random bit sequences." (See text book passage cited in the section below bearing the heading "Re: Final Action, Page 8, First Full Paragraph."

Claim 26

Point 1

Claim 26 recites receiving an encrypted message EM1, and de-crypting EM1 using K1.

The Office Action treats the encrypted hash value of the digital cash in Yacobi as the EM1. However, as explained above, in general, it is impossible to de-crypt a hash value. And the Office Action has not shown otherwise.

Again, the hash value is a type of abstract, or abbreviation, of a piece of data. For example, a hash value of a person's name may be the initials. In the case of the undersigned attorney (Gregory A. Welte), the initials, or hash value, are GAW. The name Gregory A. Welte cannot be de-crypted from the hash value.

Therefore, in general, a hash value is not reversible. It cannot be de-crypted to provide the original message. Thus, the claimed de-crypting of EM1 is not found in Yacobi.

Point 2

The claim states that K1 is the key used to perform the de-cryption. No such K1 is used to de-crypt the hash value of the

09/651,979
Art Unit 2137
Docket No. 8490

digital cash in Yacobi.

Point 3

The discussion of claim 21, above, applies here. There is no de-cryption of an encrypted response using K1 in the references.

Point 4

No valid teaching has been given for combining the references. The combined references do not produce a true "random bit sequence."

Claim 27

Claim 27 recites:

27. Method according to claim 26, and further comprising:

- d) in connection with the second transaction,
 - i) receiving into the portable computer an encrypted message EM2 from the external terminal, and
 - ii) de-crypting EM2 using K2.

EM2 and K2 have not been shown in Yacobi.

The comments regarding claim 26 apply here.

No valid teaching has been given for combining the references. The references do not produce a random bit sequence.

Claim 28

Point 1

Claim 28 states that a PDA "has no secure area."

Yacobi states that his device is "tamper-resistant." (Column 5, lines 18, 19.)

Yacobi thus teaches against these types of recitation. If a user can gain access to memory from which the seeds are derived, the device containing that memory is not "tamper resistant" as required by Yacobi.

Point 2

No valid teaching has been given for combining the references. The references do not produce a random bit sequence.

Claim 30

Claim 30 states that an apparatus "has no secure area."

Yacobi states that his device is "tamper-resistant." (Column 5, lines 18, 19.)

Yacobi thus teaches against these types of recitation. If a user can gain access to memory from which the seeds are derived, the device containing that memory is not "tamper resistant" as required by Yacobi.

No valid teaching has been given for combining the references. Contrary to the PTO's motivation, the references,

either singly or together, do not produce "random bit sequences."

Claim 32

Claim 32 recites receiving an encrypted message, and de-crypting it using key K1. As explained above, in connection with claim 21, the only possible "encrypted message" in Yacobi is the hash value. But that has been encrypted using a bank's "private key." (Column 10, lines 22 - 25.) Thus, the "session key" of Yacobi is not used to de-crypt that hash value.

Further, as explained above, no reason has been given as to why Yacobi's customer would want to de-crypt the hash value, and Yacobi does not state that the customer does so. Only a merchant receiving the digital cash associated with the hash value would want to de-crypt the hash value.

Further still, no valid teaching has been given for combining the references. They do not produce "random bit sequences."

Claim 33

No valid teaching has been given for combining the references. They do not produce "random bit sequences."

As explained above, Menezes teaches against the claim, in teaching that the source of the "seed" must be kept secret. The claim states that the source is not secret.

Claim 38

Point 1

Claim 38(f) recites encrypting M using key K1. The PTO asserts that the hash value, or the digital cash, in Yacobi shows M. However, as explained above, if encryption of either of those occurs, the encryption uses the bank's private key. (Column 10, lines 22 - 25.)

That private key cannot correspond to the claimed K1, because K1 was received in encrypted form from the portable computer.

Further, the claim states that M(encrypted) is de-crypted using K1. That cannot occur in Yacobi, because any K1, even if present, will not de-crypt something encrypted by the bank's private key.

Point 2

No valid teaching has been given for combining the references. The motivation to "generate a random bit sequence" cannot be a teaching, because the references cannot do that, alone or together.

RESPONSE TO OBVIOUSNESS REJECTIONS OF CLAIMS 35 - 37

Claims 35 - 37 were rejected as obvious, based on Yacobi, Menezes, and Kawan.

Point 1

These claims state that the portable computer requires a PIN "and will not complete the transaction without the PIN."

Kawan, paragraph 30, is cited to show this recitation.

However, that paragraph states that Kawan's ATM may require a PIN. The paragraph states:

. . . the automated teller machine verifies the smart card 20 within the personal data assistant 22.

The user may be required to input . . . a PIN.

Upon completion of the verification, the user can then perform transactions . . . through the personal data assistant 22 . . .

This indicates that the PIN is entered into the ATM, not into the PDA. One reason in support of this conclusion is the very last phrase in the passage above. That phrase implies that the preceding "verification" (including PIN entry) was handled by the ATM, because the phrase states that now, after the verification, the customer can utilize the PDA. That implies that the PDA was not used for the verification.

In any case, Kawan's paragraph 30 is at least ambiguous as to whether the PIN is entered into the PDA or the ATM. That is insufficient as a showing under section 103.

Point 2

No teaching has been given for combining the references. The rationale given is "to verify the user." (Office Action, page 5, top.) However, several problems reside in this rationale.

Problem 1

The claims state that a PIN is entered into the "portable computer." You can "verify the user" in Kawan by entering the PIN into the ATM. Thus, the stated motivation does not lead to the claimed recitation of entering the PIN onto the "portable computer."

Problem 2

Numerous ways exist to "verify a user." A PIN is just one. The Office Action has not shown why a particular mode of verification (a PIN) should be used in pursuing the stated goal (verifying the user).

Problem 3

The combination of references is contrary to Yacobi.

Yacobi discusses an ATM. (Column 5, line 35.) Everybody knows that ATMs require PINs to be entered onto the ATM's keypad. Thus, Yacobi teaches entering a PIN onto an ATM keypad.

The PTO's citation of Kawan as showing claims 35 - 37 is

contrary to this teaching. Thus, even if Kawan does teach that the PIN should be entered into the portable computer, which Appellant disputes, Kawan's teaching is contrary to Yacobi.

The PTO must provide an explanation overcoming this contradiction.

Problem 4

The PTO's position is contrary to Yacobi for another reason.

Yacobi discusses verification of the user, at column 9, line 10 et seq. Yacobi undertakes a two-step process. First, he accepts data from the digital wallet. (Column 9, line 10 - 16.) Then, he verifies the user "using traditional methods." (Column 9, lines 16 - 18.)

Plainly, "traditional methods" imply requesting a PIN be entered into the ATM.

Therefore, Yacobi teaches against the claimed entry of a PIN into the portable device.

REBUTTAL OF FINAL ACTION'S "RESPONSE TO ARGUMENTS"

Appellant addresses the "Response to Arguments" beginning on page 5 of the Final Office Action as follows.

Primary Point

The "Response to Arguments" fail to negate the previous

09/651,979
Art Unit 2137
Docket No. 8490

Arguments given in this Brief.

Re: Final Action, Paragraph Spanning Pages 5 and 6

This paragraph is a one-sentence listing of descriptions of Appellant's arguments. Appellant does not admit to the accuracy of the descriptions, and the listing does not rebut Appellant's arguments.

Re: Final Action, Page 6, First Full Paragraph

This paragraph, in essence, states that Yacobi encrypts every message transmitted using the session key, in the transaction wherein the customer downloads digital cash.

However, no proof of this statement is given. Appellant has examined Yacobi, and can find no such statement in Yacobi.

Further, the statement is incorrect. Yacobi, column 10, lines 6 - 36, discusses downloading digital cash to the customer's wallet. That cash is a message. It is not encrypted.

Further still, the statement is incorrect for another reason. Yacobi encrypts the hash value using the bank's private key. (Column 10, lines 22 - 25.) That is directly contrary to the PTO's statement.

Further still, even if the statement is correct, it does not show the claim recitation in question. The claim states "decrypting the encrypted response using the plain text of K1."

09/651,979
Art Unit 2137
Docket No. 8490

The PTO relies on the "hash value" of the "digital cash" to show the claimed "encrypted response." But the "hash value" is not "de-crypted" "using the plain text of K1," as claimed. There is no reason for the customer to de-encrypt the encrypted hash value, and Yacobi does not state that the customer does so.

Appellant repeats a passage previously set forth in this Brief:

Claim 21(c) recites "de-crypting the encrypted response using the plain text of K1." The Office Action cites Yacobi, column 9, line 65 - column 10, line 31 to show this.

POINT 1

However, that passage of Yacobi shows generating digital cash by a bank. The digital cash is described in column 10, lines 14 - 16, and an example of a 550-bit number is given.

Yacobi then states that a hash value is derived from the 550-bit number. The bank then encrypts the hash value, using its private key. (Column 10, lines 22 - 25.) The encrypted hash value is then transferred to the customer's electronic wallet. (Column 10, lines 32, 33.)

Applicant points out that no decryption occurs in this passage of Yacobi. Claim 21(c) recites a de-crypting process.

Thus, the encrypted hash value of Yacobi does not correspond to the "encrypted response" in claim 21(c). That encrypted hash value is not decrypted, as claimed.

Re: Final Action, Page 6, Last Full Paragraph

This paragraph merely asserts that Yacobi shows de-crypting. That is insufficient to show the claims.

In the last sentence, this paragraph states that Yacobi was not relied on to show "determining the original value of the hashed information." This statement is directly contrary to the Final Action, page 3, end of first paragraph, which states that Yacobi's hash value is the "encrypted response" which is de-crypted.

If the hash value is de-crypted, then the "original value" of the hash value is determined, contrary to the PTO's assertion on page 6, last paragraph.

If Yacobi's digital cash is relied on to show the "encrypted response," then Appellant points out that (1) it appears that Yacobi does not encrypt the digital cash and (2) even if he did, there is no reason for the customer to de-crypt it. The merchant to whom the digital cash is given as payment would perform the de-cryption.

Re: Final Action, Page 7, First Full Paragraph

This paragraph first makes an assertion which is not proven, namely, that "every message" is encrypted in Yacobi.

Proof is required. And it has been demonstrated elsewhere herein that the assertion is incorrect.

Then this paragraph concludes from the assertion that the

09/651,979
Art Unit 2137
Docket No. 8490

"coins 70" are encrypted. But Yacobi does not state that the coins are encrypted.

Proof is required. The latter statement (regarding encryption of the "coins 70") cannot be based on an unproven assertion.

Re: Final Action, Page 7, Second Full Paragraph

This statement asserts that the encrypted hash value of Yacobi is de-crypted. But no proof is given.

Re: Final Action, Paragraph Spanning Pages 7 and 8

This paragraph asserts facts which have not been shown in Yacobi.

The argument of this paragraph is addressed in POINT 5, above, under claim 21.

Further, the argument given does not support the conclusion. The conclusion is that Yacobi's de-cryption of the hash value is done within the electronic wallet. But the assertions at the top of page 8 of the Final Action do not support that conclusion.

Further still, the argument pre-supposes that the hash value was encrypted in the first place, and thus requires de-cryption by the electronic wallet, so that the merchant can use the hash value. But none of this has been shown in Yacobi. The merchant can perform the de-crypting, not the wallet.

Re: Final Action, Page 8, First Full Paragraph

This paragraph asserts that a motivation exists to use the random number generation of Menezes to create the keys of Yacobi.

Appellant responds: Why ? A reason is required. Yacobi has his own approaches for generating his keys. Why does he need the approach of Menezes ?

Further, as explained above, Menezes discusses several different approaches. Not all those approaches produce the claimed invention. A teaching is required for selecting the approach which produces the claimed invention. No such teaching has been given.

The last sentence of this paragraph asserts that "Menezes produces **random** keys." The PTO previously made a similar argument, to which Appellant responded in his previous Appeal Brief, mailed on January 23, 2006. That response is repeated here:

**2.8 RANDOM AND PSEUDO-RANDOM SEQUENCE
GENERATION**

. . . .

Of course, it is impossible to produce something truly random on a computer.

. . . any random-number generator on a computer . . . is, by definition, periodic.

Anything that is periodic is, by definition, predictable.

And if something is predictable, it can't be random.

A true random-number generator requires some random input; a computer can't provide

09/651,979
Art Unit 2137
Docket No. 8490

that.

(Applied Cryptography, page 44, by Bruce Schneier (John Wiley & Sons, New York, 1996, ISBN 0 471 12845 7)).

Re: Final Action, Page 9, First Paragraph

This paragraph fails to provide a teaching for selecting the elements from Menezes which produce the claimed invention.

Appellant also respectfully submits that this paragraph must contain typing errors, because it makes no sense. The paragraph states

Menezes teaches that it is best to use multiple sources to obtain [the] best random numbers . . .

Appellant submits that this makes no sense. Precisely **HOW** does one use "multiple sources" to obtain a random number ? And why is one random number "better" than another ?

Further, some of those multiple sources are contrary to the claimed recitation of using data in user-accessible memory. Thus, Menezes teaches away from the claim.

Re: Final Action, Page 9, Second Paragraph

Point 1

The conclusion of this paragraph does not follow from the premises. The conclusion is that Menezes lacks a teaching against storing the records in user accessible memory.

But that conclusion is directly contrary to Menezes express teachings. Part of the Brief, above, is repeated here:

Menezes, in section 5.2, states that "A random bit generator requires a . . . source of randomness." Under claim 21, the "source of randomness" would be the claimed "records." Thus, under claim 21, the "source of randomness" would be "user-accessible."

But Menezes' section 5.2 also states, "The generator must not be subject to observation." Menezes is contrary to storing the "records" in "user-accessible memory," as claimed.

Thus, Menezes teaches against claim 21.

Also, Menezes' section 5.2(ii) lists some events which may be similar to those in the "records" of claim 21. But Menezes states that an "adversary" should be prevented from "observing" those events. (Menezes, section 5.2(ii), fourth sentence.) Again, that is opposite to claim 21, which states that those events are stored in "user-accessible memory."

Point 2

This paragraph of the Final Action fails to explain how the "adversary" (or absence thereof) contradicts these express teachings of Menezes.

It may be that the PTO is arguing something like this:

PTO's Supposed Argument

Menezes teaches keeping the seed-sources secret, because he does not want adversaries to see the seed-sources.

However, Appellant's invention does not face

09/651,979
Art Unit 2137
Docket No. 8490

the problem of adversaries, so that the teachings of Menezes regarding secrecy do not apply.

However, several problems exist in this Supposed Argument.

PROBLEM 1

The PTO has not shown that Appellant faces no "adversaries." If no adversaries are present, why does Appellant perform encryption ?

PROBLEM 2

The Supposed Argument is illogical. The Supposed Argument first combines the references, and then compares the combination to the claimed invention. The Supposed Argument then (incorrectly) finds that the claimed invention lacks "adversaries." Thus, the Supposed Argument concludes, the teachings of Menezes regarding secrecy can be ignored, because no adversaries are present.

This approach is illogical because the initial combination of references does not produce the claimed invention in the first place. The combination does not contain seeds in "plain view," that is, in user-accessible memory, because Menezes teaches against that.

Thus, this approach never produces something which matches the claim. Consequently, one never reaches the step of recognizing that the claimed invention supposedly lacks adversaries.

PROBLEM 3

The Supposed Argument is using Appellant's claims as part of the teaching for combining the references. That is, the absence of an "adversary" is inferred from the claims. And the absence is used to eliminate a teaching of Menezes.

That is not allowed. MPEP § 706.02(j) states:

Contents of a 35 U.S.C. 103 Rejection

. . .
The teaching or suggestion to make the claimed combination . . . must . . . be found **in the prior art** and not based on applicant's disclosure.

PROBLEM 4

As just explained, the absence of "adversaries" must be shown in the prior art. Then it must be shown how that absence contradicts the teachings of Menezes in favor of secrecy.

That has not been done.

Re: Final Action, Page 9, Third Paragraph

This paragraph fails to rebut Appellant's counter-example. Computer memory is not required to generate a seed, if one uses real-time incoming data. As another example, one can measure temperature or wind velocity every hour, minute, second, or whatever, and use those measured values as the seed. Those

09/651,979
Art Unit 2137
Docket No. 8490

measured values need not be stored, and then recalled for later use as the seed.

Re: Final Action, Paragraph Spanning Pages 9 and 10

If Menezes states that the software approach is "more difficult," then that is a teaching away.

If the overall discussion of Menezes somehow contradicts that teaching-away, then the Board of Appeals must interpret Menezes' teachings accordingly.

Re: Final Action, Page 10, First Full Paragraph

The paragraph fails to rebut Appellant's argument. Yacobi shows two, or more, embodiments. At least one embodiment, if combined with Menezes, fails to show the claimed invention.

A teaching is required in favor of selecting the embodiment which the PTO chose for combination with Menezes.

Re: Final Action, Page 10, Second Full Paragraph

This paragraph is incorrect.

The PTO previously stated that the hash value of Yacobi qualifies as the "encrypted response" which is de-crypted using the plain text of K1. (Final Action, page 3, end of first paragraph.) That is directly contrary to this present Second Full Paragraph on page 10.

Re: Final Action, Paragraph Spanning Pages 10 and 11

"EM2" is an encrypted message, which is received.

The Final Action has still not identified such a message.

If it is a second encrypted hash value, received in a second transaction, then it does not fall under the claim language, as explained herein. For example, it cannot be de-crypted using K2, because it was encrypted using Yacobi's bank's private key.

Appellant requests that "EM2" be specifically identified, by column- and line number, in Yacobi.

Re: Final Action, Page 11, First Full Paragraph

Appellant points out that MPEP § 2111 states:

**PRIOR ART MUST BE CONSIDERED IN ITS ENTIRETY,
INCLUDING DISCLOSURES THAT TEACH AWAY FROM THE
CLAIMS**

A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention.

Therefore, the PTO's concept that it can selectively rely on favorable parts of a reference, and ignore other parts, is invalid.

09/651,979
Art Unit 2137
Docket No. 8490

Re: Final Action, Page 11, Second Full Paragraph

And

Re: Final Action, Paragraph Spanning Pages 11 and 12

The PTO is interpreting a figure of Kawan. However, the discussion in the Brief, above, indicates that the PIN is entered into the ATM, not the PDA.

But even if the PTO is correct, then different approaches for entering the PIN are found in the references. The PTO has not shown a teaching for selecting one, and ignoring the others.

Re: Final Action, Page 11, Third Full Paragraph

Point 1

This paragraph is relying on the content of Appellant's claim to supply a motivation to combine references. The claims are, under section 112, part of the Specification.

MPEP § 706.02(j) states:

. . .
The teaching or suggestion to make the claimed combination . . . must both be found in the prior art and not based on applicant's disclosure.

Thus, Appellant's claim cannot be used to supply a motivation.

Point 2

This paragraph states that the PIN "can be" used for identification purposes. That does not show the claims, which

09/651,979
Art Unit 2137
Docket No. 8490

state that the system "will not complete the transaction without the PIN." Restated: the claim does not state that the claim is used for ID purposes.

Point 3

This paragraph, last sentence, states:

The mere fact that there can possibly be other methods of verification does not render the motivation improper.

Appellant respectfully points out that this sentence completely misses the point regarding a teaching for combining references.

The very existence of the "other methods of verification" means that a teaching is required for selecting **the specific method** used to show the claim recitation, to the exclusion of the other methods.

Re: Final Action, Page 12, First Full Paragraph

This paragraph fails to rebut Appellant's arguments.

Further, the characterization of Kawan as an "improvement" over Yacobi does not remove the requirement of a teaching for combining those two references.

Further still, no definition for the term "improvement" has been given, so the term is, at present, meaningless.

Still further, even if it be true that the combination

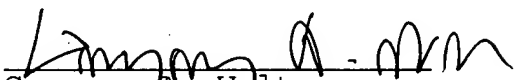
09/651,979
Art Unit 2137
Docket No. 8490

"improves the Yacobi reference," that is not a teaching under section 103.

CONCLUSION

Appellant requests that the Board overturn the rejections, and pass all claims to issue.

Respectfully submitted,


Gregory A. Welte
Reg. No. 30,434

NCR Corporation
1700 South Patterson Blvd.
WHQ - 4
Dayton, OH 45479
July 13, 2007
(937) 445 - 4956

ATTACHMENTS: 1) Claims Appendix
is 2) Statement that no related proceedings appendix
attached
3) Statement that no evidence appendix is attached

8. CLAIMS APPENDIX

21. A method of operating a portable computer, comprising:

- a) storing records of events experienced by the computer in user-accessible memory within the computer;
- b) using one or more of the records as seed for generating plain text of a first session key K1; and then
- c) encrypting K1, transmitting K1(encrypted) to an external terminal, receiving an encrypted response from the external terminal, and de-crypting the encrypted response using the plain text of K1.

22. Method according to claim 21, and further comprising:

- d) repeating processes of paragraphs (a) and (b) to produce a second session key K2, different from the first session key K1; and
- e) using K2 in a transaction with an external terminal.

23. Method according to claim 21, wherein the records used as seed include at least one element selected from the following group:

- 1) recorded button selections,
- 2) recorded pointer movements,
- 3) recorded data entered by a user,
- 4) current date setting, and
- 5) current time setting.

24. A method, comprising:

- a) using a portable computer to
 - i) generate a first session key K1, based on one or more seeds derived from data contained in user-accessible memory;
 - ii) encrypt K1 into K1(encrypted), using a public key PK;
 - iii) transmitting K1(encrypted) to an external terminal in connection with a first transaction;
- b) using the portable computer to
 - i) generate a second session key K2, based on one or more seeds derived from data contained in user-accessible memory;
 - ii) encrypt K2 into K2(encrypted), using a the public key PK;
 - iii) transmitting K2(encrypted) to an external terminal in connection with a second transaction.

25. Method according to claim 24, wherein the data from which as the seeds are derived include at least one element selected from the following group:

- 1) recorded button selections,

- 2) recorded pointer movements,
- 3) recorded data entered by a user,
- 4) current date setting, and
- 5) current time setting.

26. Method according to claim 24, and further comprising:

- c) in connection with the first transaction,
 - i) receiving into the portable computer an encrypted message EM1 from the external terminal, and
 - ii) de-crypting EM1 using K1.

27. Method according to claim 26, and further comprising:

- d) in connection with the second transaction,
 - i) receiving into the portable computer an encrypted message EM2 from the external terminal, and
 - ii) de-crypting EM2 using K2.

28. A method, comprising:

- a) maintaining a commercially available Personal Digital Assistant, PDA, which has no secure area for storing an encryption key usable to encrypt outgoing data; and
- b) using the PDA for encryption and transmission

of a message to an external controller in connection with a financial transaction.

29. Method according to claim 28, wherein the encryption comprises

- a) deriving a seed from data stored in user-accessible memory; and
- b) deriving a session key from said seed, which session key is used in the financial transaction, and not used thereafter.

30. Apparatus, comprising:

- a) a portable computer having
 - i) no secure area for storing an encryption key used to encrypt outgoing data;
 - ii) system memory, all of which is accessible to a user of the computer; and
 - iii) data stored in the system memory, which data changes over time;
- b) means for
 - i) utilizing selected changing data in the system memory as a seed for generating a session key K1;
 - ii) encrypting K1 into K1(encrypted); and
 - iii) transmitting K1(encrypted) to an

external terminal.

31. Apparatus according to claim 30, wherein the data used as the seed includes at least one element selected from the following group:

- 1) recorded button selections,
- 2) recorded pointer movements,
- 3) recorded data entered by a user,
- 4) current date setting, and
- 5) current time setting.

32. Apparatus according to claim 31, and further comprising:

c) means for

- i) receiving an encrypted message from the external terminal, and
- ii) de-crypting the encrypted message using K1.

33. A portable computer, comprising:

- a) means for storing records of events experienced by the computer in user-accessible memory within the computer;
- b) means for using one or more of the records as a seed for generating an encryption key; and
- c) means for using the encryption key in a transaction

with an external terminal.

34. Method according to claim 33, wherein the records used as the seed include at least one element selected from the following group:

- 1) recorded button selections,
- 2) recorded pointer movements,
- 3) recorded data entered by a user,
- 4) current date setting, and
- 5) current time setting.

35. Method according to claim 21, wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete the transaction without the PIN.

36. Method according to claim 24, wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete the transaction without the PIN.

37. Method according to claim 26, wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to encryption, and will not complete the transaction without the PIN.

38. A method, comprising:

- a) storing records of events experienced by a portable computer in user-accessible memory within the computer;
- b) using one or more of the records as a seed for generating a session key K1;
- c) encrypting K1 into K1(encrypted) using a public key;
- d) transmitting K1(encrypted) to an external terminal;
- e) at the external terminal, de-crypting K1(encrypted) into K1;
- f) encrypting a message M into M(encrypted) using K1 as key;
- g) transmitting M(encrypted) to the portable computer; and
- h) decrypting M(encrypted) using K1 within the portable computer.

09/651,979
Art Unit 2137
Docket No. 8490

9. EVIDENCE APPENDIX - NONE

09/651,979
Art Unit 2137
Docket No. 8490

10. RELATED PROCEEDINGS APPENDIX - NONE